Filed 10/28/24

Page 1 of 16

2

3

4

5

The MDL and JCCP Plaintiffs and Defendants (the "Parties") desire to expedite the production of Device Data from the forensic images of Bellwether Plaintiff Main Devices in an efficient way, which would allow Defendants and their forensic experts to fully analyze the usage data from those Devices while preventing the disclosure of substantive "User Generated" content to Defendants without prior review by Plaintiffs. Consistent with those objectives, the Parties submit this Stipulated Proposed Device Data Protocol and Order (the "Protocol") for entry by the Court. The undersigned parties, by and through their attorneys in both the MDL and JCCP proceedings, hereby stipulate as follows:

1. **DEFINITIONS**

For the purposes of this protocol:

- "Action" shall refer to the actions consolidated in MDL No. 3047 and JCCP 5255, 1.1. including any other action hereafter added or transferred to these consolidated proceedings, and all actions later remanded to their respective transferor courts.
- 1.2. "Bellwether Counsel" means counsel representing a specific Bellwether Plaintiff as well as their support staff (including but not limited to attorneys, paralegals, secretaries, law clerks, and investigators), who are not employees of a Party to the Action but are retained and have appeared in this Action to represent or advise a Party to this Action.
- 1.3. "Bellwether Plaintiff" refers to any one of the currently selected MDL personal injury bellwether plaintiffs (12) or JCCP personal injury bellwether plaintiffs (21) existing at the time of this Order.
- 1.4. "Defendants" means any of the named defendants in the JCCP or MDL, either individually or collectively, inclusive of any employees or staff of the companies themselves as well as any and all outside counsel representing these companies.
- 1.5. "Device Usage Data" is all of the data from Bellwether Plaintiffs Main Devices outlined below in this Stipulated Proposed Device Data Protocol and Order, which Plaintiffs are producing to the Defendants' Forensic Experts for their technical analyses. Device Usage Data consists of the forensic artifacts like data and metadata that reflect user actions, device

- 1.6. "ESI Protocol" refers to the ESI protocol entered in MDL 3047 at Doc. 690.
- "Forensic Experts" refers to iDiscovery Solutions ("IDS")² and FTI Consulting 1.7. Technology ("FTI"), the forensic vendors Defendants have engaged to perform the technical analyses on the Device Usage Data from the Bellwether Plaintiffs' Main Devices. If Defendants engage additional Forensic Experts, those experts will be disclosed to Plaintiffs and will also execute the Protective Order.
- 1.8. "Main Device" means "[A]ll devices (cellphones, tablets, laptops, computers, and the like) which are in each Bellwether PI Plaintiff's possession, custody, or control and that they have habitually, routinely, or regularly used during the relevant time period to access the Defendants' platforms." DMO 8 at 8:24–9:25. For the MDL PI Bellwether Plaintiffs, Main Device refers to those devices identified by Plaintiffs in the Main Device Spreadsheet for which a full filesystem ("FFS") image was performed. For the JCCP Plaintiffs, these are the devices identified by Plaintiffs on the ESI Data Source list.

1

9

10

11

12

13

14

15

16

17

18

19

20

21

23 24

25

26

¹ The Parties are aware that addressing, phone numbers, usernames, account names, and handles are metadata fields that, under traditional eDiscovery mechanisms, would only be produced in relation to responsive ESI, but that it is inefficient to segregate these metadata fields for the purposes of this protocol. However, if Defendants plan to use the content of these metadata fields for substantive purposes, then Defendants will inform Plaintiffs so that the Parties may meet and confer.

²⁷

² IDS is retained only by YouTube. As such, IDS will only receive Redacted Forensic Extractions for Main Devices of Plaintiffs who have named YouTube as a Defendant.

4

6

7

10

13 14

15 16

17

18 19

20

21 22

23

24

25 26

27

28

³ See, 1.5 "Device Usage Data" and 1.12 "User Generated" supra.

- 1.10. "Redacted Forensic Image/Extraction" means a complete forensic copy of a Main Device, from which all media files (audio, photo, and video files) have been excised. In the case of computers (Windows and Mac), the Redacted Forensic Images will include unallocated space addressed in Section 6.2 infra.
- 1.11. "Substantive User Content" means any User-Generated text or media that reveals the substance, purport, or meaning of the item. For files, Substantive User Content includes any User-Generated text or multimedia. For communications, Substantive User Content includes any User-Generated file name, subject, message body, or viewable multimedia attachment. For web browsing, Substantive User Content includes any part of a URL beyond the domain (a path that discloses the specific section or page of website, and any cached or locally stored text or multimedia). Substantive User Content includes User-Generated content the user created for communication, sharing, or storage purposes as well as text searchable data or reviewable media or logs cognizable as having been generated by the Bellwether Plaintiff or any other individual, that could be construed to convey information, including the user's or others' thoughts, actions, or intentions. Examples of Substantive User Content include User Generated content of: text messages, emails, chats, any other electronic communications, photos, camera rolls, audio, videos, chats, caller information, medical or financial information, calendars, contacts, folder or file names, any portion of the URL beyond the domain or User Generated text within browser histories or note taking applications, and documents such as spreadsheets, PDFs or Microsoft Word Documents, the identities of third-parties with whom the user communicated. Substantive User Content does not include metadata, unless the user created the content of the metadata, as with file name metadata.³
- 1.12. "User Generated" or "User-Generated" as used in this Protocol, means any text that was intentionally generated by the Bellwether Plaintiff to convey the substance, purport, or meaning of the item and was not automatically generated by the device or any of its applications.

2. SCOPE

The limitations and protections regarding Substantive User Content imposed by this Protocol and Order do not cover: (a) any information that is in the public domain at the time of production to the Forensic Experts or becomes part of the public domain after its production to the Forensic Expert as a result of publication not involving a violation of this Order or any Order in either MDL 3047 or JCCP 5255, including becoming part of the public record through trial or otherwise; and (b) any information obtained by the Defendants after the disclosure from a source who obtained the information lawfully and under no obligation of confidentiality to the Plaintiffs. This document does not address the use of Device Usage Data at trial.

3. **DURATION**

Even after final disposition of this Action, the confidentiality obligations imposed by this Order remain in effect until Plaintiffs agree otherwise in writing or a court order otherwise directs. Final disposition shall be deemed to be the later of (1) dismissal of all claims and defenses in this Action, with or without prejudice; or (2) final judgment of the Action after the completion and exhaustion of all appeals, rehearings, remands, trials, or reviews, including the time limits for filing any motions or applications for extension of time pursuant to applicable law and the time limits for filing a petition for writ of certiorari to the Supreme Court of the United States if applicable. The Court shall retain jurisdiction to enforce or modify this Order and to make further orders with respect to the use or confidentiality designations of Device Data.

4. NO WAIVER AND EXECUTION OF PROTECTIVE ORDER

4.1 To the extent that the Forensic Experts have direct or indirect access to information protected by attorney-client privilege, the work product doctrine, or other privilege or legally-recognized protection from discovery, such disclosure will not result in any waiver of privilege or protection.

4.2 The Experts shall sign Exhibit A to the Confidentiality Agreement and Protective Order (the "Protective Order"), filed separately in this case, and be bound to the Protective Order as modified herein. The Expert shall be allowed to engage or hire other outside support as necessary

to comply with this Order, so long as the outside support also signs and agrees to be bound by the Protective Order as modified herein.

5. REDACTION OF SUBSTANTIVE USER CONTENT

- 5.1 Relevant and responsive Substantive User Content from the Main Devices is being produced separately by Plaintiffs in accordance with the ESI Protocol entered in this litigation.
- 5.2 If the Forensic Experts are unable to determine whether data encountered constitutes Substantive User Content and want to disclose it to Defendants, Defendants will meet and confer with Plaintiffs as to whether the category of data may be disclosed to Defendants. Plaintiffs will promptly respond to such conferral within five business days, such that Defendants may promptly address any disagreement with the Court.
- 5.3 The Forensic Experts are prohibited from disclosure of Substantive User Content to Defendants and are required under this protocol to redact or otherwise exclude all Substantive User Content from any reports, analyses, or other disclosure in any form to Defendants, absent agreement from Plaintiffs or an Order from the Court.
- 5.4 Disclosure of Substantive User Content by the Forensic Experts without Plaintiffs' prior review or consent is strictly prohibited. If Substantive User Content is inadvertently disclosed, Defendants will promptly notify Plaintiffs and the Parties shall meet and confer within 5 business days to discuss what steps, if any, are necessary to address the inadvertent disclosure. Defendants shall not use any improperly disclosed Substantive User Content absent agreement from Plaintiffs or an Order from the Court.
- 5.5 The Forensic Experts may convey to Defendants the fact that they have found Substantive User Content on the Redacted Forensic Images/Extractions and what category of Substantive User Content they have found, so long as the Forensic Experts do not identify the substance of that Substantive User Content to Defendants without Plaintiffs' authorization.
- 5.6 If the Forensic Experts contend Substantive User Data must be disclosed to Defendants for any reason, including because it cannot be redacted or is necessary for the Forensic Experts' technical analyses of Plaintiffs device usage, Defendants must meet and confer with Plaintiffs and

22

23

24

25

26

give Plaintiffs the opportunity to review the Substantive User Content for privilege or other legally cognizable protections. Plaintiffs will promptly respond to such conferral within five business days, such that Defendants may promptly address any disagreement with the Court. Productions by the Forensic Experts of Substantive User Content from the Main Devices shall include identifying information, such that the Forensic Experts' production could be correlated with other productions from the same device. The identifying information will include the following data fields: Custodian Name, Device Make and Model, Serial Number (or IMEI), Extraction Method, and Device Time Zone.

5.7 If the Substantive User Content identified in 5.6 is Substantive User Content previously reviewed and produced by Plaintiffs from the same device, the Forensic Experts may incorporate that Substantive User Content previously produced to Defendants in their reports and analyses.

5.8 Where the data or investigation by the Forensic Experts supports such a request, Defendants shall have the right to request, in writing, that Plaintiffs review and disclose responsive Substantive User Content that may be identified by the Forensic Experts, that would not have otherwise been the subject of prior productions from the traditional ESI sources within these devices. The request to Plaintiffs shall include the reason(s) the data or investigation supports such a request. Defendants must meet and confer with Plaintiffs and give Plaintiffs the opportunity to review the Substantive User Content for privilege or other legally cognizable protections. Plaintiffs will promptly respond to such conferral within five business days, such that Defendants may promptly address any disagreement with the Court.

5.9 Upon receipt of a request for Substantive User Content that Plaintiffs choose to review, Bellwether Counsel will have FIVE business days to review and produce the relevant and responsive data. If Bellwether Counsel believes it cannot review and produce data within that time period, it will notify Defendants immediately and the Parties shall meet and confer in good faith to discuss the length of time necessary for Bellwether Counsel to complete this pre-production review for privilege and responsiveness.

27

24

25

26

5.10 The Forensic Experts shall maintain the Redacted Forensic Images/Extractions in a secure location and shall not produce copies of them or any subset of such ESI, to anyone else except as necessary to comply with this Order. Accordingly, all ESI that has been produced pursuant to this Order shall be treated by the Forensic Expert and any receiving parties as if the Plaintiffs had designated them CONFIDENTIAL and subject to the Protective Order.

6. PRODUCTION OF DATA

6.1 Unless otherwise stipulated to by the parties below, or as ordered by the Court, Plaintiffs shall produce to the Forensic Experts—for their eyes only—the entirety of the full filesystem extraction or forensic image, after removal of all multimedia data (i.e., photos, images, video, and audio). Plaintiffs agree to produce the associated metadata for the removed media unless, as outline above, the content was User Generated.⁴

6.2 Defendants acknowledge that media files (audio, photo, and video files) may exist within the Redacted Forensic Images/Extractions and unallocated space on computers, notwithstanding reasonable efforts by Plaintiffs to remove such media files. For example, media files may be carved or exist within unredacted archive files. When accessing or processing unallocated space or unredacted archives on computers, the Defendants' Forensic Experts shall not utilize tools or viewers to view media files that may exist (or fragments of which may exist). Nonetheless, if Defendants' Forensic Experts encounter media files, they will treat any such media files as Confidential Data, and will not disclose its substance to Defendants.

- 6.3 Plaintiffs shall produce Redacted Forensic Extractions for mobile devices (*e.g.*, phones) in Cellebrite Reader (UFDR) format.
- 6.4 Plaintiffs shall produce Redacted Forensic Images of computers (Windows and Mac) as industry standard redacted physical forensic images.

⁴ See, 1.5 "Device Usage Data" and 1.12 "User Generated," supra.

⁵ A purpose of this provision is to prevent the Defendant Forensic Examiners from inadvertently uncovering CSAM which may exist in the unallocated space of the Main Devices.

Document 1284 Filed 10/28/24

Page 14 of 16

Case 4:22-md-03047-YGR

Document 1284 Filed 10/28/24

Page 15 of 16

Case 4:22-md-03047-YGR

Document 1284 Filed 10/28/24

Page 16 of 16

Case 4:22-md-03047-YGR